DLA PIPER US LLP
ROY K. MCDONALD, Bar No. 193691
roy.mcdonald@dlapiper.com
STEVE CHIARI, Bar No. 221410
stephen.chiari@dlapiper.com
DAVID M. DOYLE, Bar No. 233439
david.doyle@dlapiper.com
153 Townsend Street, Suite 800
San Francisco, California 94107-1957
Tel: 415.836.2547
Fax: 415.659.7447

T. WADE WELCH & ASSOCIATES
CHAD M. HAGAN (*application for admission pro hac vice filed concurrently herewith)*
chagan@twwlaw.com
CHRISTINE D. WILLETTS (*application for admission pro hac vice filed concurrently herewith)*
cwilletts@twwlaw.com
2401 Fountainview, Suite 700
Houston, Texas 77057
Tel: 713.952.4334
Fax: 713.952.4994

Attorneys for Plaintiffs
DISH NETWORK L.L.C., ECHOSTAR TECHNOLOGIES L.L.C. and NAGRASTAR L.L.C.

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

DISH NETWORK L.L.C., a Colorado Limited Liability Company, ECHOSTAR TECHNOLOGIES L.L.C., a Texas Limited Liability Company, and NAGRASTAR L.L.C., a Colorado Limited Liability Company,

Plaintiffs,

v.

SatFTA aka SERGEI ALEX ALEXEYEV,

Defendant.

CASE NO. CV 08 1561 PVT

PLAINTIFFS' COMPLAINT FOR:

1) **Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1);**
2) **Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2);**
3) **Violation of the Communications Act of 1934, as amended, 47 U.S.C. § 605(a);**
4) **Violation of California Penal Code § 593d(a);**
5) **Violation of California Penal Code § 593e(a);**
6) **Violation of California Penal Code § 593e(b);**

DEMAND FOR JURY TRIAL

Plaintiffs DISH NETWORK L.L.C., ECHOSTAR TECHNOLOGIES L.L.C. (collectively "EchoStar"), and NAGRASTAR L.L.C. ("NagraStar"), by their undersigned counsel, file this Original Complaint against the above-named Defendant and state as follows:

INTRODUCTION & NATURE OF THE ACTION

1. Plaintiffs EchoStar and NagraStar bring this action against Defendant SatFTA aka Sergei Alex Alexeyev ("Defendant") for unlawfully manufacturing, distributing, and otherwise trafficking in devices, components, and technology intended to facilitate the illegal and unauthorized reception and decryption of EchoStar's subscription and pay-per-view television programming.

2. EchoStar is a multi-channel video provider, providing video, audio, and data services to customers throughout the United States, Puerto Rico, and the U.S. Virgin Islands via a Direct Broadcast Satellite ("DBS") system. EchoStar uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment services ("Programming") to consumers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price).

3. EchoStar operates its DBS Programming under the trade name "DISH Network." To provide customers with a variety of Programming channels, EchoStar continues to contract and purchase the distribution rights of copyrighted Programming from providers such as network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other content providers.

4. Because EchoStar generates revenues through the sale of subscription packages and pay-per-view programming, and because the ability to attract and retain the distribution rights for Programming is dependent upon preventing the unauthorized reception of DISH Network Programming signals, all of EchoStar video channels, except for certain promotional channels, are digitally secured.

5. EchoStar protects DISH Network Programming from unauthorized viewing by using a management and security system ("Security System"), which serves two interrelated functions: (1) subscriber-management—allowing EchoStar to "turn on" or "turn off"

Programming that a customer ordered, cancelled, or changed; and (2) encryption—preventing individuals or entities who have not purchased DISH Network Programming from viewing it.

6. The Security System is comprised of two parts. First, EchoStar encrypts (electronically scrambles) its satellite signals using proprietary technology provided by NagraStar. Essentially, NagraStar provides EchoStar with "smart cards" ("Access Cards") that contain a microprocessor component that functions as a security computer to a "conditional access system" known as Digital Nagra Advanced Security Process ("DNASP"). These Access Cards are utilized in the satellite receivers that customers either purchase or lease. Second, the DNASP uses a complex encryption system that is combined with a Digital Video Broadcasting ("DVB") scrambler/encoding system to effectively protect and encrypt DISH Network Programming.

7. Defendant violated federal and state law by offering to the public, providing, or otherwise engaging in the traffic of codes, devices, components, and technology that are primarily designed to circumvent and/or defeat Plaintiffs' Security System and ultimately facilitate the unauthorized reception of EchoStar's encrypted satellite signals and DISH Network Programming.

PARTIES

8. Plaintiff DISH NETWORK L.L.C. is a Colorado limited liability company with its principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado 80112.

9. Plaintiff ECHOSTAR TECHNOLOGIES L.L.C. is a Texas limited liability company with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112.

10. Plaintiff NAGRASTAR L.L.C. is a Colorado limited liability company with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112. NAGRASTAR is a joint venture between ECHOSTAR and the Kudelski Group, a group of companies headquartered in Switzerland.

11. Upon information and belief, Defendant SatFTA aka Sergei Alex Alexeyev ("SatFTA") is a California resident residing at 558 Los Olivos Drive, Santa Clara, California.

JURISDICTION AND VENUE

12. This is a civil action predicated upon violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*, the Communications Act of 1934, as amended, 47 U.S.C. § 605 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2511 *et seq.* Therefore, jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331, 1338, 47 U.S.C. § 605(e)(3)(A), 17 U.S.C. § 1203, and 18 U.S.C. § 2520(a). The Court has supplemental jurisdiction over the state law claims asserted herein pursuant to 28 U.S.C. § 1367(a).

13. Personal jurisdiction and venue are proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(1) because Defendant resides within this judicial district, 1391(b)(2) because a substantial part of the events giving rise to this action occurred in this judicial district, 1391(b)(3) because Defendant may be found in this judicial district and is subject to *in personam* jurisdiction, and 1400(a) because this case asserts the infringement and circumvention of protected copyright materials.

INTRADISTRICT ASSIGNMENT

14. Intra-district assignment to the San Jose Division of the United States District Court for the Northern District of California is appropriate under Civil Local Rules 3-2(c) and 3-2(e) because a substantial part of the events or omissions that give rise to the claims alleged herein occurred in the County of Santa Clara, California.

PLAINTIFFS' SECURITY SYSTEM[1]

15. A consumer wishing to subscribe to and receive DISH Network Programming must first have the necessary equipment, which consists primarily of: (1) a satellite dish antenna ("dish"); (2) an integrated receiver/decoder ("receiver" or "set-top box"); and (3) a credit card-sized ECHOSTAR Access Card.

16. A satellite dish can be mounted on a rooftop, deck railing, or other structure at the subscriber's home or business. After proper installation, the dish antenna will receive

[1] Plaintiffs' allegations as to themselves and their own actions are based upon personal knowledge. Based upon reasonable and diligent investigative efforts, Plaintiffs believe that substantial evidentiary support exists for the allegations related to the Defendant herein or that such allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and/or discovery

programming signals from one of EchoStar's satellites, which are then transmitted by wire into the set-top box. The receiver processes and descrambles the incoming signal using the data and encryption technology stored in the v Access Card. The Access Card is loaded into the receiver through a slot located at the face of the unit.

17. EchoStar provides the Access Cards to customers for use with the receivers for the purpose of enabling authorized access to DISH Network Programming. Absent a subscription to DISH Network, EchoStar will not provide a consumer an Access Card or authorize access to encrypted DISH Network Programming. Subscribers are not authorized to modify or tamper with the Access Card, which are clearly marked as property of EchoStar and must be returned upon request.

18. The EchoStar Access Card is essential to the operation of the set-top box because it contains a secure embedded microprocessor that essentially functions as a small security computer, with secret keys and software that contain technology codes ("Nagra Software") used to communicate with the receiver and enable the descrambling of DISH Network Programming. The Nagra Software and the security components contained in each set-top box are licensed from NagraStar.

19. The Nagra Software within each Access Card is supported by two code segments of memory: (1) Read-Only-Memory ("ROM"); and (2) Electronically Erasable Programmable Read-Only-Memory ("EEPROM"). Generally, the ROM code segment contains the intimate knowledge and information regarding Plaintiffs' Security System and how it works; whereas the EEPROM code segment contains the secret keys enabling the decryption of EchoStar's satellite signal.

20. The ROM code segment provides detailed instructions and commands to EchoStar Access Cards and set-top boxes in the normal operation of Plaintiffs' Security System. Access to the proprietary information stored in the ROM code is necessary to unlock the safe containing the secrets to Plaintiffs' Security System.

21. The EEPROM code segment stores data and command codes that have been written to EchoStar Access Cards which the ROM code reads from to perform its calculation and

operation functions. Moreover, the EEPROM code segment contains secret "transmission" keys and secret "pairing" keys (collectively known as "security keys"). The security keys are used to encrypt and decrypt the communications between the EchoStar Access Card and the set-top box.

22. EchoStar communicates with the microprocessor in each Access Card by sending and receiving satellite signals which are routinely updated. The information transmitted to and temporarily stored on the Access Card includes the most recent security keys and software necessary to view DISH Network Programming.

23. At the first activation of a customer's subscription, EchoStar sends a signal to the smart card in order to "pair" or "marry" the smart card to the receiver. Both smart card and receiver have a unique identification number that is maintained by EchoStar's subscriber management system. This pairing operation utilizing the two unique identification numbers is mandatory for the proper operation of the Security System because certain secrets are contained in both the smart card and the set-top box.

24. One of the most important secrets contained in the set-top box are the DES keys (also called Box Keys), which are integral to the process of pairing a set-top box to an individual Access Card. These Box Keys are unique and individual to one, and only one, receiver. Once they are imprinted from the Receiver to the Smart card - done during the process of the first communication between EchoStar and the individual Receiver - they form the only "language" of communication that can be used for the Receiver to decrypt certain crucial information sent by EchoStar to the Receiver.

25. EchoStar added a JTAG port on the bottom of EchoStar's satellite receivers for use in the manufacturing process to load test software into the satellite receiver. The test software gets loaded into memory on the receiver and runs software diagnostic, among other things, on the satellite receiver's memory board and makes the receiver go through certain test paces while another computer on the outside of the receiver is checking patterns and telling the receiver to go to the next test. For example, the computer diagnostic that is run through the JTAG port tells the EchoStar satellite receiver to decode certain audio, test computer and satellite receiver functions, all the while doing this simultaneously. The JTAG port is also used by EchoStar in its service

organization when EchoStar gets a satellite receiver back and needs to clean it up and send it back out to the field. Importantly, there is absolutely no other legitimate use for this JTAG port. Specifically, the only use a non-EchoStar individual would have for these JTAG ports would be to 'pirate' a receiver.

26. The TSOP is part of the memory within the chip and it holds the "box key." The box key is used to identify whether a given card goes with a particular receiver. The box key functions as a pairing key and is used for communication from the smart card to the receiver. Essentially, each EchoStar receiver's unique Box key is a receiver-specific language that facilitates communication from a satellite signal to the receiver via the smart card. Because an EchoStar receiver's box key is fundamental in protecting the DISH Network programming from satellite piracy, these box keys are known only to authorized EchoStar personnel. Accordingly, when an authorized satellite receiver is added to the DISH Network system, based upon that receiver's identification, EchoStar knows what the secret box key is that is stored in that particular receiver's memory, and that is the key that will be used to de-scramble the messages from the smart card. EchoStar looks up the authorized user's identification number and can them determine the box key assigned to that receiver. Then, EchoStar's up-link center sends the secret number in an encrypted message to the authorized receiver's smart card so that the smart card will have the same key number in it. It is this process that allows the encrypted messages in the DISH Network signal to be sent from the smart card to the authorized receiver.

27. Plaintiffs' Security System effectively controls access to the copyrighted materials that comprise DISH Network Programming. In addition, the Security System ensures that the protection afforded to such copyrighted works, such as limitations on the dissemination and use in accordance with EchoStar's contractual agreements with content providers, is preserved.

THE PIRACY OF DISH NETWORK PROGRAMMING

28. Various types of equipment and devices appear on the black market for the sole purpose of illegally descrambling or "pirating" EchoStar Programming. These devices initially consisted of printed circuit boards that when programmed, operated in the place of, and/or in conjunction with, DISH Access Cards. These devices compromised the DISH Security System

by modifying and/or circumventing the security software in the DISH Access Cards. In addition to the various pirate devices, certain software, codes, commands, updates, patches, "fixes", and other technology support information is used to assist in the unlawful circumvention of EchoStar's security system and the resulting theft of EchoStar's programming.

29. EchoStar and NagraStar have developed anti-piracy divisions in an effort to combat the theft of EchoStar's programming. EchoStar's anti-piracy strategy includes the periodic introduction of new generations of DISH Access Cards containing updated software that the pirates have not yet hacked. The first DISH Access Card was known as the ROM 2 card. EchoStar and NagraStar subsequently deployed DISH Access Cards with improved anti-piracy technologies, including the ROM 3, ROM 10, ROM 11, ROM 101, ROM 102, ROM S01, ROM S02 and ROM 206.

30. The main purpose of developing and introducing successive generations of DISH Access Cards is to foil hackers and render obsolete existing piracy devices. Converting EchoStar customers to new generations of DISH Access Cards and switching the satellite datastream so that it can only be received by the new DISH Access Cards requires the pirates to start over again in attacking the technology. EchoStar and NagraStar have invested and continue to invest significant time and money in these enhancements. EchoStar and NagraStar also update the DISH Access Cards to improve their functionality and service to EchoStar's customers.

31. EchoStar and NagraStar also invest heavily in developing and deploying countermeasures to maintain the integrity of the DISH Security System. Such countermeasures include electronic countermeasures ("ECM's"), which are periodically broadcast over the satellites to disable unauthorized DISH Access Cards.

32. Despite these improvements to the DISH Security System, piracy has continued to proliferate. Concurrently with the introduction of new generations of DISH Access Cards, new sophisticated piracy devices and components thereof ("Pirate Boards") have appeared on the black market. These devices include so-called "AVR Boards" which are printed circuit boards containing a microprocessor, a parallel port connector, and a socket for a DISH Access Card, which permit a DISH Access Card to be inserted into the socket and the AVR board itself inserted

into the receiver. The AVR board microprocessor can be programmed with piracy software to enable the receiver to descramble EchoStar Programming. Newer versions of Pirate Boards can even be programmed and used without a DISH Access Card.

33. Other devices available on the black market include "programmers" and "loaders" whose only known purpose is to enable hackers to re-program and modify DISH Access Cards and Pirate Boards to circumvent the DISH Security System. These types of devices are particularly damaging to EchoStar because an individual with such a device can: (1) repeatedly modify a DISH Access Card, (2) modify numerous DISH Access Cards, and re-sell them to other persons, and (3) program and/or modify Pirate Boards to steal EchoStar Programming.

34. Piracy software is an essential component of most piracy devices. Among the software offered on piracy web sites today is software that is created and offered solely for the purpose of "programming", "cracking", "flashing" and "modifying" DISH Access Cards, receivers, or Pirate Boards, or "repairing", "patching", or "fixing" illegally-modified DISH Access Cards, receivers, or Pirate Boards that have been disabled by ECM's. This software is known by such names as "NagraEdit", "rf040", "BAPA_BELL", "Space Twister" and "ROM Tier Maker." Piracy web sites often restrict access to piracy software to persons who pay fees to become "members" or "subscribers".

35. Pirates often refer to the use of modified DISH Access Cards, Pirate Boards, or hardware as "testing" (implying that they are used for the purpose of "testing" the Receiving Equipment). EchoStar does not authorize anyone to modify, alter, reprogram or "test" its Receiving Equipment for any purpose whatsoever. Legitimate subscribers to EchoStar would have no reason to "test", tamper with, or alter the Receiving Equipment. Rather, the sole purpose of such activities would be to circumvent the DISH Security System to steal EchoStar Programming.

36. Some piracy devices are sold pre-programmed with piracy software. However, in an effort to avoid prosecution, many satellite pirates offer only "unprogrammed" or "unflashed" piracy devices for sale to consumers. In such cases the pirates will suggest that the piracy devices they offer for sale are "legitimate" or "legal" because the purchaser must obtain piracy software

from other sources and program them before they can be used for piracy. Pirates will generally refer their customers to sources of software components either verbally, by e-mail or by way of links to software providers' web sites.

37. Many pirates also offer services in support of the piracy devices and the piracy software that they sell. These services include:

(a) access card programming services by which DISH Access Cards are re-programmed by pirates to permit them to be used for piracy purposes;

(b) box key "extraction" services by which Box Keys are obtained from receivers, to be used in "pairing" the receivers to DISH Access Cards supplied by pirates; and

(c) "unlocking" services by which receivers and DISH Access Cards that have been "paired" together can be "unlocked", thereby permitting the receiver or DISH Access Card to be used with a DISH Access Card or receiver other than the one to which it has been "paired"

38. The ongoing provision of new versions of piracy software and the aforementioned services results in continual losses for EchoStar.

39. The black market in Piracy Technology represents a multimillion-dollar industry in Canada and the United States. The pirates who fuel this black market are geographically dispersed and typically operate individually or within a very small group. Pirates can start up businesses with a minimal investment of capital and other resources, and typically operate as "fly-by-night" businesses with few assets and are able to shut down or relocate with ease. By using the Internet, pirates are able to operate without regard to national borders and reach millions of potential customers. The identities of pirates who develop, manufacture, and distribute Piracy Technology are known only to a few. Locating their places of business and web sites is often a difficult and time-consuming undertaking.

40. Pirates are generally aware of the illegal nature of their activities, and often take steps to avoid detection and to conceal the evidence of their wrongdoing. For example, pirates who operate retail storefront premises often keep little inventory in the premises, with the balance being stored at storage facilities, in neighbouring businesses, or at their residences or those of their relatives or associates. Pirates who operate Internet-based businesses benefit from the

anonymity which the Internet provides, and often locate the servers containing their web sites' databases in undisclosed (and sometimes offshore) locations, and use third party on line payment processors that store their sales records elsewhere. Pirates can access their web sites by "remote access" from their residences, and in many cases orders received by their web sites are automatically e-mailed to the pirates or their associates who can invoice, package and ship the orders from wherever the Piracy Technology is being stored

FORUM & CHAT WEB SITES

41. Many pirates also operate or participate in piracy web sites that serve as a "forum" for the dissemination and exchange of information pertaining to Piracy Technology and satellite piracy generally. In some cases, forum sites do not sell any Piracy Technology themselves. Rather, they provide information and instruction on the use of Piracy Technology and provide links to other piracy web sites that sell Piracy Technology and related services to permit consumers to unlawfully obtain EchoStar's programming.

42. It is typical for forum sites to receive advertising revenue from other piracy web sites that place advertisements or links on them. Alternatively, some pirates operate forum sites to establish credibility in the piracy community and obtain a loyal group of users who they then refer to other web sites operated by that pirate to purchase Piracy Technology.

43. Among the software offered on these "forum" sites today is software that is created and offered solely for the purpose of "programming", "cracking", "flashing", "fixing", or "updating" illegally modified DISH Access Cards, receivers or Pirate Boards that have been disabled by an ECM.

DEFENDANTS' WRONGFUL CONDUCT

44. At various times during the 2001-2006 timeframe, SatFTA developed and publically distributed certain Piracy Codes and Software for the purpose of circumventing, and facilitating others in circumventing Plaintiffs' security system. This section of Plaintiffs' Complaint sets forth in known detail the names and descriptions of SatFTA's Piracy Codes and Software. Plaintiffs are informed and believe that discovery will yeild evidence of additional piracy files created and distributed by SatFTA and expressly reserve their rights to supplement,

modify and/or amend their Complaint and claims against SatFTA as necessary.

45. **IRDr.exe:** SatFTA developed and publically distributed a piracy file known as IRDr.exe. This program is used to extract proprietary data from Plaintiffs' software contained within an ECHOSTAR receiver or IRD. Specifically, IRDr.exe reads the secret encryption keys (known as "box keys" that are stored in the flash memory of Plaintiffs' IRD's. These encryption keys are used by pirates to program a pirate smartcard device to receive unauthorized programming. There is no reason that any of Plaintiffs' legitimate subscribers would need knowledge of these encryption keys and/or how to extract them from Plaintiffs' IRD's.

46. Defendant's IRDr.exe program is utilized to extract the firmware from Plaintiffs' IRD's using the JTAG port. Once the firmware has been extracted and copied from the IRD to a personal computer, the box keys and other encryption keys can be copied or modified to create unauthorized IRD clones. The encryption keys are also used in other piracy programs, such as NagraEdit, which allows for the unauthorized modification of Plaintiffs' IRD's.

47. Defendant's IRDr.exe program also contains a location ID calculator. The location ID is a piracy countermeasure that was designed by EchoStar to combat unlawful account packing. Accounting packing is a form of customer fraud where IRD's from different households are placed onto the same account. This activitiy allows multiple receivers to be placed on an existing account at a $5 incremental cost instead of a full subscription charge of $25-100 per account. Plaintiffs' discovery of, and investigation into, unauthorized account packing is dependent on the secrecy of the algorithm used to generate the location ID checksums. Defendant's IRDr.exe program allows a pirate to calculate legitimate location ID values, thereby eliminating location ID as an investigative tool for account packing fraud.

48. **IRDcM.exe:** Defendant also engaged in the development and distribution of a piracy file known as IRDcM.exe. This file provides the ability to determine which channels and tiers are available on the different satellites used in EchoStar's DISH Network platform. IRDcM.exe works by examining proprietary data in the satellite receiver. This channel/tier information is then used in programs that modify EchoStar smartcards, such as "wBinInfo", and other piracy devices which are used to steal EchoStar's encrypted programming.

49. Defendant's IRDcM.exe program works by utilizing the JTAG port on Plaintiffs' IRD's to access the memory RAM of the IRD while it is in use. By gaining unauthorized access to the table contained in the IRD's RAM, pirates can update, modify and/or re-program their illegal smartcards to circumvent Plaintiffs' ECM's launched to disable the very devices that Defendant's program allows them to reprogram. There is no legitimate purpose for an authorized EchoStar subscriber to have access to this information – which is used by pirates solely for the purpose of stealing Plaintifffs' encrypted programming.

50. **i2c.jpg:** Defendant also developed and distributed a piracy diagram known as i2c.jpg. This diagram details the electrical circuitry for interfacing to the memory of an EchoStar IRD. Essentially, i2c.jpg is a blueprint for building a connector to interface with the IRD's EEPROM. There is customer-specific information stored inside the EEPROM, such as channel lists and remote configuration. The EEPROM also contains evidence of ECM's launched by Plaintiffs to disable various circumvention devices which are used to steal EchoStar's encrypted programming. Pirate devices built using Defendant's i2c.jpg diagram allow hackers to erase the digital evidence contained within the EEPROM used in Plaintiffs' IRD's – which, in turn, allows the pirates to circumvent the security measures implemented by Plaintiffs to protect its signal from unauthorized receiption and decryption.

51. **jm.gif:** Defendant also developed and distrubited a piracy diagram called jm.gif. This diagram discloses proprietary information relating to the layout of Plaintiffs' security software. Jm.gif details the exact location of critical data secured within Plaintiffs' IRD memory, including the memory location of various encryption and cryptographic keys used to secure communications between Plaintiffs' IRD and smartcards.

52. **Jtag-pcb2.bmp:** Defendant also developed and distributed a piracy file known as jtag-pcb2.bmp. This file discloses proprietary information about the layout of EchoStar's hardware and details the circuitry lawywout required to interface with the software of EchoStar's IRDs. With this diagram, pirates can build a device to interface with Plaintiffs' software and allo them to download that software (as well as uploading new versions of that software) for use in circumventing ECM's launched by Plaintiffs to disable pirate devices.

53. In addition to the foregoing, Plaintiffs are informed and believe that Defendant developed and distributed, and/or assisted in the development and distribution of the following piracy-related files: list501-4sectors.c, bind522, DNLview, getfw, getSDT, info.c, stc721.c, BindKeyMaker, csum, DE, DNLlist, FindR00, GetTable, IRDcm, LSPC, ParseEMMstream, PVRdFormat, PVRExplorer, TSRPP, CnTrList, DishUpgrade, DishVuEPG, FlashEdit, 12Clog, IDread, jtag_r, jtag_2, mEEP. These files, combined with the other files identified above in this section of Plaintiffs' complaint, are hereinafter collectively referred to as "Pirate Codes and Software".

54. Defendant distributed the aforementioned Piracy Codes and Software on various hacker websites including: www.innermatrix.com (and innermatrix chat forum); www.interestingDevices.com (and interesting devices chat forum). Defendant published these Piracy Codes and Software to facilitate and/or otherwise assist others in the circumvention of Plaitntiffs' security system and the unauthorized receiption and decryption of Plaintiffs' copyrighted programming. Defendant's Piracy Codes and Software was downloaded hundreds of times for use by EchoStar pirates. More specifically, upon information and believe, Defendant's posts and files were downloaded for use by pirates and hackers as follows: jvc-00AB-BJCA-11JN-756P.bin (43 downloads); PVR50x-17DB-DCTA-10SN-P067-7D06.bin (512 downloads); jtag-pcb2.bmp (2,734 downloads); IRD Jtag 101 thread (6,287 messages); jtag8.zip (1,986 downloads); irdr.3.5.14.21.zip (71 downloads); irdr.3.5.12.21.zip (1,428 downloads); irdr.3.4.12.18.zip (1,849 downloads); irdr.3.3.11.12.zip (1,547 downloads); irdr311.zip (914 downloads); i2c.zip (786 downloads); PVRdRip1003.zip (427 downloads); pvrdrip.zip (525 downloads); pvrdinfo.zip (421 downloads); listc_141cs2.sat.csv (944 downloads); channeltable0109.txt (409 downloads); channeltable0101.txt (541 downloads); channeltabledp301p157.txt (184 downloads).

FEDERAL RAID EXECUTED AT SatFTA'S RESIDENCE & SUBSEQUENT EVIDENCE ANALYSIS

55. On March 31, 2006, United States federal agents executed a raid and search warrant at SatFTA's residence. Following execution of the raid, the federal agents notified

Plaintiffs of the true identify of the individual using the internet alias SatFTA – Defendant Sergei Alex Alexeyev.

56. During the raid the agents seized, among other items, 9 computer hard drives, 12 EchoStar smartcards and 20 EchoStar IRD's (satellite receivers). The FBI and United States' Attorneys Office provided Plaintiffs with an opportunity to inspect and analyze the seized materials through proper chain-of-custody requests. Based on that analysis, Plaintiffs discovered the following:

(a) 13 of the EchoStar IRD's contained patent modifications including, *inter alia*, unauthorized pins mounted to the circuitry boards, and unauthorized cables and/or wires soldered to contacts contained in the circuitry boards. Four of these IRD's also contained coding in the non-volatile memory that was left as a result of the units being "hit" by one of Plaintiffs' ECM's which targeted illegally modified receivers. Seven of the IRD's also contained additional evidence of unauthorized modifications including holes drilled into the chassis and damage done to the JTAG contacts of the receivers;

(b) 4 additional EchoStar receivers were seized which contained unauthorized software modifications including modifications to the cryptography keys, boot software and main software which allow the receivers to circumvent EchoStar's security system and gain access to programming that the receivers were not authorized to receive. One of these IRD's (R0028552448) was modified to match the boot software of another EchoStar receiver thereby creating an unauthorized "clone" which was capable of receiving all of the information, data and programming which was sent to, or authorized to be received by, the original receiver.

57. Defendant was also observed (and admitted to) using illegally modified EchoStar IRDs and smartcards to circumvent Plaintiffs' security system and steal the copyrighted DISH Network programming.

///

///

///

///

CLAIMS FOR RELIEF

COUNT I

(Manufacture of and Traffic in Signal Theft Devices, Components, and Technology in Violation of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(1))

58. Plaintiffs incorporate by reference paragraphs 1 through 57 as if set forth herein.

59. Defendant was and is actively engaged in the business of manufacturing, using, importing, offering to the public, providing, or otherwise trafficking in illegal pirate codes, software, devices, components, and technology in violation of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1).

60. The Pirate codes, software, technology and software provided by Defendant is: (1) designed or produced by Defendant primarily for the circumvention of Plaintiffs' Security System—a technological measure that effectively controls access to, copying and distribution of, copyrighted works; (2) made available by Defendant despite having no limited commercially significant purpose or use other than to circumvent Plaintiffs' Security System; and/or (3) posted, distributed or otherwise disseminated by Defendant, or through others acting in concert, with knowledge that the Pirate codes, software, technology and software are used to circumvent Plaintiffs' Security System.

61. Defendant was and is manufacturing, using, importing, offering to the public, providing, or otherwise trafficking in the Pirate Codes and Software with knowledge that these devices, components, and technology are used to circumvent and defeat Plaintiffs' conditional access technological measures that protect the copyrighted works on the DISH Network satellite platform.

62. Defendant's actions that constitute violations of the DMCA were performed without the permission, authorization, or consent of ECHOSTAR, NAGRASTAR, or any owner of copyrighted Programming broadcast on the DISH Network platform.

63. Defendant violated sections 1201(a)(2) and 1201(b)(1) of the DMCA willfully and for purposes of commercial advantage or private financial gain.

///

64. Defendant's misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the Court, Defendant will continue to violate the alleged provisions of the DMCA.

COUNT II

(Manufacture of and Traffic in Signal Theft Devices, Components, and Technology in Violation of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(2))

65. Plaintiffs incorporate by reference paragraphs 1 through 64 as if set forth herein.

66. Defendant was and is actively engaged in the business of manufacturing, importing, offering to the public, providing, or otherwise trafficking in illegal pirate codes, software, devices, components, and technology in violation of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. §§ 1201(a)(2).

67. The Pirate codes, software, technology and software provided by Defendant is: (1) designed or produced by Defendant primarily for the circumvention of Plaintiffs' Security System—a technological measure that effectively controls access to, copying and distribution of, copyrighted works; (2) made available by Defendant despite having no limited commercially significant purpose or use other than to circumvent Plaintiffs' Security System; and/or (3) posted, distributed or otherwise disseminated by Defendant, or through others acting in concert, with knowledge that the Pirate codes, software, technology and software are used to circumvent Plaintiffs' Security System.

68. Defendant was and is manufacturing, importing, offering to the public, providing, or otherwise trafficking in the Pirate Codes and Software with knowledge that these devices, components, and technology are used to circumvent and defeat Plaintiffs' conditional access technological measures that protect the copyrighted works on the DISH Network satellite platform.

69. Defendant's actions that constitute violations of the DMCA were performed without the permission, authorization, or consent of ECHOSTAR, NAGRASTAR, or any owner of copyrighted Programming broadcast on the DISH Network platform.

///

70. Defendant violated sections 1201(a)(2) of the DMCA willfully and for purposes of commercial advantage or private financial gain.

71. Defendant's misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the Court, Defendant will continue to violate the alleged provisions of the DMCA

COUNT III

(Facilitating the Unauthorized Decryption and Reception of Satellite Signals in Violation of the Communications Act, 47 U.S.C. § 605(a))

72. Plaintiffs incorporate by reference paragraphs 1 through 71 as if set forth herein.

73. Defendants conduct was and is assisting others, namely those downloading, copying, using and/or otherwise re-distributing the Piracy Codes and Software developed and published by SatFTA, to intercept and receive ECHOSTAR's encrypted satellite transmissions without authorization and for their own benefit in violation of 47 U.S.C. § 605(a).

74. Defendant was and is assisting, directly or indirectly, with the design, manufacture, development, assembly, modification, solicitation, and/or distribution of Pirate Codes and Software used to circumvent EchoStar's security system with knowledge, or having reason to know, that such devices and technology are used primarily to assist in the unauthorized interception and decryption of direct-to-home satellite services in violation of 47 U.S.C. § 605(a).

75. Defendant violated 47 U.S.C. § 605(a) of the Communications Act willfully and for the purpose of direct or indirect commercial advantage or private financial gain.

76. Defendant's misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the Court, Defendants will continue to violate the alleged provisions of the Communications Act.

COUNT IV

(California Penal Code § 593d(a))

77. Plaintiffs incorporate by reference paragraphs 1 through 76 as if set forth herein.

78. Defendant violated California Penal Code § 593d(a) by knowingly and willfully: (1) making or maintaining unauthorized connections to EchoStar's DBS system or Plaintiffs'

Security System, or any components thereof; (2) purchasing, possessing, attaching, causing to be attached, assisting others in attaching, or maintaining the attachment of unlawfully reprogrammed EchoStar Access Cards or other Signal Theft Devices to EchoStar's DBS system or Plaintiffs' Security System; (3) making or maintaining any modification or alteration to EchoStar Access Cards without authorization from EchoStar; or (4) obtaining and using unlawfully reprogrammed EchoStar Access Cards or other Signal Theft Device to obtain EchoStar Programming without authorization.

79. EchoStar is a "multichannel video or information provider" within the meaning of California Penal Code § 593d(i).

80. Defendant's acts constituting violations of California Penal Code §§ 593d(a)(1)-(4) have been and continue to be performed without the permission, authorization, or consent of Plaintiffs.

81. Defendant's violations have injured, and will continue to injure, Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, infringing Plaintiffs' trade secrets and proprietary information, and interfering with Plaintiffs' contractual and prospective business relations.

82. Defendant's violations of California Penal Code §§ 593d(a)(1)-(4) were done knowingly and willfully, and for the purpose of commercial advantage or private financial gain. EchoStar is entitled to recover, under California Penal Code § 593d(f), the greater of three times its actual damages, or statutory damages of $5,000 for each violation of California Penal Code §§ 593d(a)(1)-(4). Plaintiffs are also entitled to recover reasonable attorneys' fees. California Penal Code § 593d(f)(2).

COUNT V

(California Penal Code § 593e(a))

83. Plaintiffs incorporate by reference paragraphs 1 through 82 as if set forth herein.

84. Defendant violated California Penal Code § 593e(a) by attaching and/or maintaining and assisting others in attaching and/or maintaining unauthorized piracy devices to

equipment used to receive and/or decrypt EchoStar's encrypted satellite broadcase television programming and/or modifying or altering EchoStar IRD's or smartcards for the purpose of intercepting, receiving or using programming or services which are not authorized by Plaintiffs and/or which are not subject to a valid subscription service with corresponding payment to Plaintiffs.

85. EchoStar is a "multichannel video or information provider" within the meaning of California Penal Code § 593d(i).

86. Defendant's acts constituting violations of California Penal Code §§ 593e(a) have been and continue to be performed without the permission, authorization, or consent of Plaintiffs.

87. Defendant's violations have injured, and will continue to injure, Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, infringing Plaintiffs' trade secrets and proprietary information, and interfering with Plaintiffs' contractual and prospective business relations.

88. Defendant's violations of California Penal Code §§ 593e(a) were done knowingly and willfully, and for the purpose of commercial advantage or private financial gain. EchoStar is entitled to recover, under California Penal Code § 593e(c), the value of the connection and subscription fees actually charged for the period of unauthorized use for each specific violation of California Penal Code § 593e(a). Plaintiffs are also entitled to recover reasonable attorneys' fees. California Penal Code § 593e(d).

COUNT VI

(California Penal Code § 593e(b))

89. Plaintiffs incorporate by reference paragraphs 1 through 88 if set forth herein.

90. Defendants violated California Penal Code § 593e(b) by knowingly and willfully providing a device, plan, or kit for a device (including but not limited to unlawfully reprogrammed EchoStar Access Cards and a methodology for hacking EchoStar's Security System) designed in whole or in part to descramble or intercept or otherwise make intelligible

EchoStar's satellite television programming transmission signal without the express authorization of EchoStar.

91. EchoStar is a "subscription television system" within the meaning of California Penal Code § 593h(1).

92. EchoStar's satellite transmission of television programming is an "encoded, scrambled, or other nonstandard signal" within the meaning of California Penal Code § 593e(g).

93. Defendants' acts constituting violations of California Penal Code § 593e(b) have been, and continue to be, performed without the permission, authorization, or consent of Plaintiffs.

94. Defendants' violations have injured, and will continue to injure, Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, infringing Plaintiffs' trade secrets and proprietary information, and interfering with Plaintiffs' contractual and prospective business relations.

95. Defendants' violations of California Penal Code § 593e(b) were committed knowingly and willfully, and for the purpose of commercial advantage or private financial gain.

96. Due to Defendants' wrongful conduct, Plaintiffs are entitled to either: (i) statutory damages in an aggregate amount of not less than $500 or more than $10,000 for each unlawful device; or (ii) three times the amount of actual damages sustained by Plaintiffs as a result of Defendants' violations of California Penal Code § 593e(b) in addition to any revenues which have been obtained by Defendants as a result of Defendants' violations thereof, or (iii) an amount equal to three times the value of the services unlawfully obtained by Defendants, or the sum of $500 for each unauthorized signal theft device manufactured, sold, used, or distributed. Cal. Penal Code § 593e(c)(2)).

97. Because Defendants' violations of California Penal Code § 593e(c) were committed knowingly and willfully and for purposes of commercial advantage or private financial gain, the Court may increase the award of damages, whether actual or statutory, by an amount of not more than $50,000. Because of Defendants' violations of California Penal Code §

593e(c) were committed knowingly, willfully, and wantonly, punitive damages are appropriate under California Penal Code § 593e(c)(2). Plaintiffs are also entitled, under California Penal Code § 593e(d), to its full costs plus an award of reasonable attorney's fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs EchoStar and NagraStar seek judgment against Defendant as follows:

A. For a grant of permanent injunctive relief restraining and enjoining Defendant, and his employees, agents, representatives, attorneys, and all persons acting or claiming to act on their behalf or under their direction or authority, and all persons acting in concert or in participation with them, from:

(1) offering to the public, providing, or otherwise trafficking in any circumvention or piracy codes, devices, software, hardware, technology, or part thereof, through any Internet website, or in any other way that:

(a) is primarily designed or produced for the purpose of circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on EchoStar's Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted Programming on the DISH Network platform;

(b) have only a limited commercially significant purpose or use other than to circumvent Plaintiffs' Security System, including the encryption and access control protection contained in the software on EchoStar's Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted Programming on the DISH Network platform;

(c) is knowingly distributed by Defendants and/or others acting in concert with Defendants for use in circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on EchoStar's Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted Programming on DISH Network; and

(2) assembling, modifying, selling, and/or distributing any satellite Receivers or Pirate Software knowing or having reason to know that such device or software is primarily of assistance in the unauthorized decryption of direct-to-home satellite services through any Internet website, or in any other way; and

(3) assisting others in receiving (including assistance offered by providing hypertext links or banner advertising) EchoStar's electronic communications without EchoStar's authorization through any Internet website, or in any other way.

B. For an Order impounding all electronic copies of Pirate Software, satellite Receivers, or other circumvention or signal theft technology, components, or devices in the custody or control of Defendants or related entities that the Court has reasonable cause to believe were involved in a violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*

C. For an Order directing Defendants to preserve and maintain all records, in any form (including electronic form), that evidence, refer, or relate to: modified satellite Receivers, Pirate Software, communications or correspondence with suppliers of software, hardware, or other equipment or know-how concerning satellite television piracy, including any dealer, distributor, or manufacturer of modified satellite receivers, pirate software or codes, or any other circumvention device or technology or part thereof.

D. Award Plaintiffs the greater of its actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of up to $100,000 for each violation of 47 U.S.C. § 605(e)(4), pursuant to 47 U.S.C. § 605(e)(3)(C)(i).

E. Award Plaintiffs the greater of its actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of up to $2,500 for each violation of 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1), pursuant to 17 U.S.C. §§ 1203(c)(2) and 1203(c)(3)(A).

F. Award Plaintiffs the greater of its actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the

amount of $100 per day for each violation of 18 U.S.C. § 2511(1) or $10,000, pursuant to 18 U.S.C. § 2520(c)(2).

G. Award Plaintiffs punitive damages afforded by law pursuant to 18 U.S.C. § 2520(b)(2), and in equity for unjust enrichment.

H. For an accounting and restitution by Defendant of all gain, profit, and advantages derived from Defendant's unlawful and unfair business acts and practices.

I. For an award of Plaintiffs' costs, reasonable attorneys' fees, and investigative fees.

J. For pre- and post-judgment interest on all profits and damages granted by this Court in accordance with the law.

K. For such other and further relief as the Court deems just and proper.

DATED: March 21, 2008

Respectfully submitted,

DLA PIPER US LLP

By: _____
DAVID M. DOYLE
Attorneys for Plaintiffs
DISH NETWORK L.L.C., ECHOSTAR TECHNOLOGIES L.L.C. and NAGRASTAR L.L.C.

DEMAND FOR JURY TRIAL

Plaintiffs DISH NETWORK L.L.C., ECHOSTAR TECHNOLOGIES L.L.C., AND NAGRASTAR L.L.C., by their undersigned counsel, hereby demand a trial by jury in this action.

DATED: March 21, 2008

Respectfully submitted,

DLA PIPER US LLP

By: _____
DAVID M. DOYLE
Attorneys for Plaintiffs DISH NETWORK L.L.C., ECHOSTAR TECHNOLOGIES L.L.C. and NAGRASTAR L.L.C.

JS 44 (Rev. 12/07) (cand rev 1-08)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON PAGE TWO OF THE FORM.)

I. (a) PLAINTIFFS
Dish Network L.L.C., Echostar Technologies L.L.C. and Nagrastar L.L.C

(b) County of Residence of First Listed Plaintiff Arapahoe County, CO
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorney's (Firm Name, Address, and Telephone Number)
Roy K. McDonald, Stephen A. Chiari, David M. Doyle
DLA Piper US LLP, 153 Townsend St., Ste. 800
San Francisco, CA 94107; (415) 836-2500

DEFENDANTS
SatFTA aka Sergei Alex Alexeyev

County of Residence of First Listed Defendant Santa Clara County, CA
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE LAND INVOLVED.

Attorneys (If Known)
(Unknown)

E-filing

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated or Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury

PERSONAL INJURY
- ☐ 362 Personal Injury — Med. Malpractice
- ☐ 365 Personal Injury — Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 444 Welfare
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities – Other
- ☐ 440 Other Civil Rights

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence

Habeas Corpus:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition

FORFEITURE/PENALTY
- ☐ 610 Agriculture
- ☐ 620 Other Food & Drug
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 630 Liquor Laws
- ☐ 640 R.R.& Truck
- ☐ 650 Airline Regs.
- ☐ 660 Occupational Safety/Health
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 730 Labor/Mgmt.Reporting & Disclosure Act
- ☐ 740 Railway Labor Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus - Alien Detainee
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA(1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☒ 490 Cable/Sat TV
- ☐ 810 Selective Service
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 875 Customer Challenge 12 USC 3410
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 892 Economic Stabilization Act
- ☐ 893 Environmental Matters
- ☐ 894 Energy Allocation Act
- ☐ 895 Freedom of Information Act
- ☐ 900 Appeal of Fee Determination Under Equal Access to Justice
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN (Place an "X" in One Box Only)

☒ 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from another district (specify) | ☐ 6 Multidistrict Litigation | ☐ 7 Appeal to District Judge from Magistrate Judgment

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing (**Do not cite jurisdictional statutes unless diversity**):
17 U.S.C. §§ 1201(a)(1), 1201(a)(2); and 47 U.S.C. § 605(a).
Brief description of cause:
Action based on manufacture/distribution of technology for illegal and unauthorized interception of TV signals.

VII. REQUESTED IN COMPLAINT:
☐ CHECK IF THIS IS A **CLASS ACTION** UNDER F.R.C.P. 23
DEMAND $ Damages TBD at trial, injunctive and other relief.
CHECK YES only if demanded in complaint: **JURY DEMAND:** ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY
PLEASE REFER TO CIVIL L.R. 3-12 CONCERNING REQUIREMENT TO FILE "NOTICE OF RELATED CASE".

IX. DIVISIONAL ASSIGNMENT (CIVIL L.R. 3-2)
(PLACE AND "X" IN ONE BOX ONLY)
☐ SAN FRANCISCO/OAKLAND ☒ SAN JOSE

DATE 3/21/08
SIGNATURE OF ATTORNEY OF RECORD